

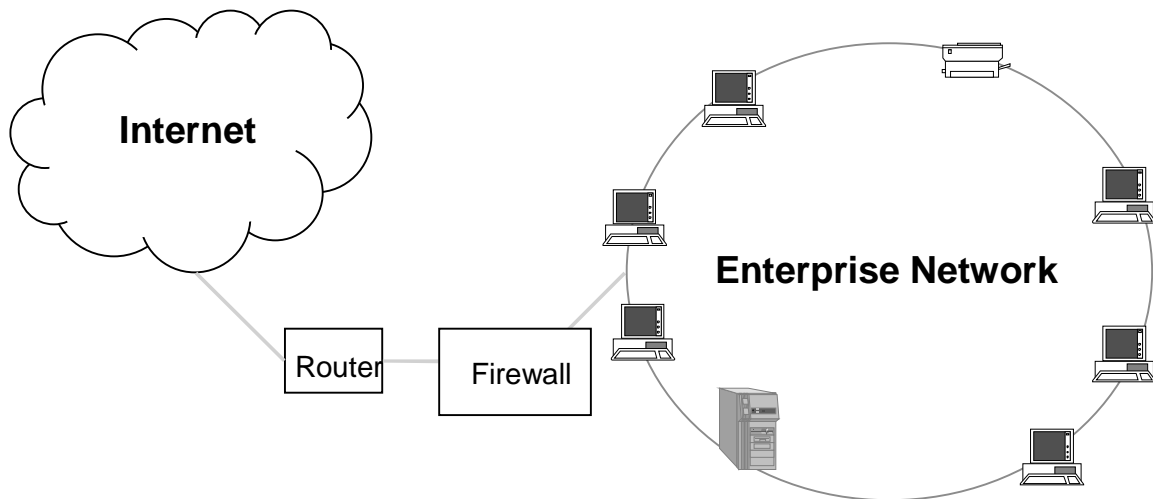
4 Business Requirements

Businesses and other organizations use the Internet because it provides useful services. Organizations choose to support (or not support) Internet-based services based on a business plan or an information technology strategic plan. In other words, organizations should analyze their business needs, identify potential methods of meeting the needs and consider the security ramifications of the methods along with cost and other factors.

Most organizations use Internet-based services to provide enhanced communications between business units, or between the business and its customers, or provide cost savings means of automating business processes. Security is a key consideration - a single security incident can wipe out any cost savings or revenue provided by Internet connectivity.

There may also be a number of different technological solutions for meeting the needs of the business, some that are more easily secured than others. Figure 4.1 shows a typical network architecture for an organization using the Internet.

Figure 4.1 Typical Internet System Architecture



The rest of this chapter explains the major services provided by Internet connectivity. It also maps the security controls available to the services they can help protect. Table 4.2 shows a mapping of security controls to the Internet-based services commonly used by businesses and organizations. The marks show which controls are most often employed to secure a given service. Some of the controls, such as incident handling, provide security for all services; the mark highlights services for which the control is essential.

Table 4.2 Mapping of Security Controls and Services

	I&A	Access Control	Firewall	Software Import Controls	Encryption	Architecture	Incident Handling	Administrative
Remote Access	X	X	X		X			X
Electronic Mail	X			X	X			X
Info Publishing		X	X			X		X
Research		X	X	X		X		X
Electronic Commerce	X	X	X	X	X	X	X	X
High Availability						X		X
Ease of Use						X		X

4.1 Remote Access

Increasingly, businesses require remote access to their information systems. This may be driven by the need for employees on travel to access email, or for sales people to remotely enter orders, or by a business decision to promote telecommuting. By its very nature, remote access to computer systems adds vulnerabilities by increasing the number of access points.

There are three major modes of remote access:

- *Service specific* remote access is typically limited to remote operation of one service, often email. Products such as Lotus Notes and cc:Mail support mobile connections to these products with no provision of general network services. This mode is generally the most secure form of operation - vulnerabilities are limited.
- *Remote Control* allows the remote user to operate a personal computer that is physically located at the corporate location. The corporate computer can be a special purpose system or the user's desktop computer. The remote computer is used strictly as a keyboard and a display. Remote control limits remote users to the software programs that are resident on the corporate computer, a plus from the security point of view. Some remote control multi-user products also provide an enhanced level of auditing and logging.
- In *Remote Node* operation, the remote computer connects to a remote access server that assigns the remote computer a network address. All operating software is located on the remote computer, along with local storage. Remote node operation provides all network services to remote users, unless access control software is utilized. Remote node operation is becoming the most popular form of remote access, but also introduces the highest level of vulnerability to corporate systems.

These forms of remote access can be accomplished using dial-in connections, telnet sessions, or using software products that support mobile computing. The following sections describe the vulnerabilities of the various methods of remote access.

4.2 Dial-in

Remote access over commercial telephone lines is still the most common form of remote access. Typically the remote computer uses an analog modem to dial an auto answer modem at the corporate location. Security methods for protecting this connection include:

- Controlling knowledge of the dial-in access numbers - this approach is vulnerable to automated attacks by “war dialers,” simple pieces of software that use auto-dial modems to scan blocks of telephone numbers and locate and log modems.
- Username/password pairs - since an attacker would need to be tapping the telephone line, dial-in connections are less vulnerable to password sniffer attacks that have made reusable passwords virtually useless over public networks. However, the use of network sniffers on internal networks, the lack of password discipline, and social engineering make obtaining or guessing passwords easy. For example, help desks are also used to dealing with legitimate users who have forgotten their passwords and will often release passwords to clever “social engineers.”
- Advanced authentication - there are many methods which can be used to supplement or replace traditional passwords. These methods include:
 - Dial-back modems - these devices require the user to enter a username/password upon initial connection. The corporate modem then disconnects and looks up the authorized remote telephone number for the connecting user. The corporate modem then dials the remote modem and establishes a connection. The user then enters the username and password for the system connection. This approach is vulnerable to call forwarding attacks, and does not provide the flexibility required to support connections from airports and hotels.
 - One Time Passwords - Cryptographic-based /response systems, such as S/Key from Bellcore, and SecurID from Security Dynamics require the user to operate a software or hardware-based password generator. These devices create a unique password for each session and require the remote user to both know the username/password information and to possess the password generator. While this method is still vulnerable to session hijacking attacks, this approach provides the minimum acceptable level of security for most remote access connections.
 - Location-based - an emerging set of authentication products takes advantage of the growing use of technologies such as the Global Positioning System to enforce location-based authentication. If a user is not connecting from an authorized location, access is denied. This technology is immature, complex and currently expensive. However, it may be appropriate for many applications. Vulnerabilities are related to the ability of an attacker to supply bogus location information. Most approaches use cryptography to prevent this form of attack.

Since most users don't hesitate to discuss sensitive matters over the telephone, dial-in connections are no less secure than the voice communications via telephone. While this is true from the confidentiality point of view, dial-in connections to computers provide an access point for intruders. These access point exist even if there is no Internet connection.

4.3 Telnet/X Windows

Telnet and the remote login commands supported by Unix provide a means for remotely logging in to computers over network connections. Many personal computers come equipped with TCP/IP software that also provides telnet capability. Telnet essentially provides a text-oriented remote control connection from the remote client to the host computer. Telnet usually requires a username/password pair be sent over the network connection in the clear - a major security weakness.

X Windows provides a remote control connection that supports use of graphical user interfaces, passing screen and keyboard data over the network connection. X Windows has a few security features that are often bypassed by users to simplify the connection process.

4.4 Mobile Computing

The use of portable computers has risen dramatically, driven by the dramatic fall in the cost, size, weight, and fragility of laptop computers. Market research firm International Data Corporation reports that in 1995, one-quarter of all computers purchased for business use were laptop computers. Most of the laptops in use by business and government agencies come configured with high speed modems, .5 GB or larger disk drives, and a variety of pre-configured communications software. A growing trend is the use of docking stations or port extenders to allow laptop computers to be used in a desktop environment as well as in out of office situations. A less common variation is the transfer of PCMCIA card-based disk drives between portable (or remote desktop-based) computers and the home office based machine.

Mobile computing involves the use of portable computers to perform business functions, and often involves establishing remote connections to corporate networks. While the connection mechanisms used are the same as described above (dial-in, telnet, etc.) the use of portable computers introduces additional vulnerabilities:

- The location of the remote computer can change frequently, often on a daily basis. Dial-back modems are generally not useful for controlling access.
- The remote computer is often used in public situations, such as on airplanes, or in airports. Data and password compromise can occur through "shoulder surfing."
- The remote computer is often left unattended in relatively insecure locations, such as in hotel rooms or in rental cars. Data stored on disk is vulnerable to snooping or copying.
- Remote computers are often lost or stolen while employees are in travel, making all information stored available to compromise. Employees are often reluctant to quickly report the loss, making fraudulent remote access possible. Some large organizations (with 4,000 or more laptop computers in use) lose on average one laptop computer per week.
- Laptop computers use internal modems for dial-in access, with the same PCMCIA card often used as the Network Interface Card when the laptop is used in an office environment. If an analog phone line is available at the desktop, the built-in modem can be used for unapproved dial-in or dial-out connections to bulletin boards or Internet Service Providers.

Mobile computing users also tend to be cellular phone users, and often discuss sensitive security-related matters over the cellular airwaves. Talking over a cellular phone is vulnerability to eavesdropping by a wide variety of criminals, competitors, and news organizations. The use of cellular or other radio-based modems for data communications increases the vulnerability level.

4.5 Electronic Mail

While the multi-media content of the World Wide Web receives most of the attention, electronic mail is what really drove the growth of the Internet. The use of Internet email to carry business-critical communications is growing exponentially. While email provides a low cost means of communicating with customers, suppliers, and partners, there are a number of security issues related to the use of electronic mail:

- Internet email addresses are easily spoofed. It is nearly impossible to be certain who created and sent an email message based on the address alone
- Internet email messages can be easily modified. Standard SMTP mail provides no integrity checking.
- There are a number of points where the contents of an email message can be read by unintended recipients. Internet email is much like a postcard - the message is viewable at every intermediate stop.
- There is usually no guarantee of delivery with Internet email. While some mail systems support return receipts, when such receipts work at all they often only signify that the user's server (not necessarily the user) has received the message.

These weaknesses make it important for organizations to issue policies defining acceptable use of electronic mail for business purposes.

4.6 Information Publishing

The Internet greatly simplifies the task of providing information to citizens, clients, suppliers, and partners - or at least those that have computers connected to the Internet. Today in the United States roughly 35% of the homes have personal computers, and only about half of those homes have the capability to connect to the Internet. It will be several years before electronic publishing can make a serious dent in paper-based publishing.

However, any use of electronic information publishing that reduces the number of requests for information via telephone or US Mail can be of significant benefit in meeting organizational goals as budgets and head counts decline. There are two primary types of information publishing, push and pull. Subscription-based magazines are an example of push publishing - information is sent to subscribers on a regular basis. Newsstand sales are an example of pull publishing - readers must take the initiative to get the information.

The electronic equivalent of push publishing is the creation of a mailing list that sends information to all subscribers of the list. Typically list server software is used to send messages to the list and to provide for adding, modifying, and deleting entries on the list. List servers are relatively secure, in that the users do not need to connect to the publishing organization's network to receive information. However, there are a few vulnerabilities:

- List server software accepts user inputs to subscribe to the list, be removed from the list, or to obtain information about the list. There is a wide variety of freeware list server software available, and some of the packages may not fully check user input. Malicious users can send Unix commands or extremely large input strings in an attempt to cause unintended operation or buffer overflows.
- If not configured correctly, list server software can make the entire list of subscriber addresses visible to each subscriber. This can provide information to support denial of service or social engineering attacks.

There are two electronic equivalents of pull publishing commonly in use on the Internet: File Transfer Protocol servers and World Wide Web servers. These have pretty much supplanted the use of bulletin board systems, although many BBS are still in use in the government.

To provide FTP services over the Internet, about all that is needed is a computer and a connection to the Internet. FTP servers can be set up on just about any computer running the Unix operating system, and on many running Microsoft Windows. Many commercial and shareware versions of ftp software are available, often as part of a TCP/IP “stack” that provides the software drivers to connect to Internet services. They can allow fully anonymous login, where passwords are not required, or they can be set up to require a valid username/password pair. FTP servers provide a simple interface resembling a standard Unix file directory. Users can retrieve files and then view or execute the files later, if they have the appropriate applications.

If an FTP server is not configured correctly, it can provide access to *any* file found on the host computer, or even on the network connected to the host computer. FTP servers should be limited to accessing a limited directory space, and should require the use of passwords whenever feasible.

Unless you've been stranded on a remote island for the past three years, you're probably familiar with the explosive growth of the World Wide Web. Web servers provide an inexpensive means of publishing information that contains text and embedded graphics, or even audio and video. The use of the HyperText Markup Language and HyperText Transfer Protocol standards allows Web-based documents to be easily retrieved and viewed by users on a wide variety of client platforms.

While developing a professional Web site is complicated and expensive, any computer connected to the Internet can be easily setup as a Web server. World Wide Web server software is available in both commercially-supported and freeware versions for all varieties of server and personal computer operating systems. Many of the latest versions of operating systems are including the software needed to host Web servers, along with very helpful “wizard” programs that automate the setup tasks.

Similar to FTP servers, Web servers can introduce significant security vulnerabilities to enterprise networks if not configured correctly. See section *WWW* for more information on security policy for Web and FTP servers.

4.7 Research

Doing research over the Internet generally involves using client software to search for and retrieve information from remote servers. Types of client software include:

- File Transfer Protocol - FTP software supports logging in to remote systems, browsing directory structures, and retrieving files.
- Gopher - Developed at the University of Minnesota, Gopher software essentially provides a graphical user interface to FTP-like browsing and retrieval functions
- World Wide Web - Web browsers have pretty much conquered the market for Internet information retrieval. Web browser client software generally includes the ability to use FTP and Gopher functions, along with more advanced multi-media capabilities.
- Proprietary systems - There are still a number of Internet-based information systems that require the use of proprietary software rather than a Web browser. These generally involve access to copyrighted or proprietary information stored in relational databases.

The major risk related to the use of the Internet for research is the possibility of importing viruses or other malicious software. With the rise of “macro viruses” that can be contained in standard word processing files, downloading documents can now be as risky as downloading executable files. In addition, the availability of “helper applications” and downloadable “applets” to support viewing of special purpose formats (such as Postscript) has increased the risk of Trojan Horse programs being hidden in legitimate programs. See the sections on Software Import and the World Wide Web for policy in this area.

A secondary risk is the “footprint” that client software leaves when used to browse Internet-based information servers. Most server software has the ability to log the IP address of the client as a minimum, and Web server software can often retrieve information on the type of browser used, the last site visited, the email address in use on the browser, and other sensitive information. In addition, Web server software can store a “cookie” file on the browser client, allowing the server to track the client’s visits to the server and keep track of what areas are visited.

4.8 Electronic Commerce

The use of computers and networks has proceeded in three major phases, or “waves” as often called by the pundits:

- Back office automation - the early days of the mainframe moved many financial and record keeping functions, such as billing, finance, and personnel, onto computers.
- Front office automation - the advent of the personal computer and local area networks allowed office functions, such as word processing, correspondence tracking, financial estimation, etc., to be taken over by computers.
- Customer contact automation - as the penetration of personal computers into business and homes advances, and the Internet continues to provide inexpensive, ubiquitous connectivity, the contact between businesses and their customers (individuals, other businesses, suppliers, partners, etc.) will more and more take place via a computer-computer connection.

This buyer to seller contact using computers and networks is the basic definition of electronic commerce. For the purposes of exploring the relevant security issues, we have broken electronic commerce into four basic classes: electronic mail, electronic data interchange, information transactions, and financial transactions. Electronic mail was discussed in detail above; the following sections address the remaining three categories.

4.9 Electronic Data Interchange

Electronic Data Interchange (EDI) is a self explanatory term. In its simplest form, EDI is the electronic exchange of information between two business concerns (referred to in the EDI world as trading partners), in a standardized format. The basic unit of exchange is a transaction set, which generally relates to a standard business document, such as Purchase Order or a Customer Invoice. Through standards bodies such as X.9 and UN/EDIFACT, the business community has developed a set of standard transactions sets for various industries.

Each transaction set has an extensive set of data elements required for that business document, with specified formats and sequences for each data element. If the transaction contains more than one transaction (many purchase orders sent to one vendor) several transaction groups would be preceded by a functional group header, and would be followed by a function group trailer.

Businesses began to use EDI to reduce the time and cost of dealing with suppliers. Driven by the automobile manufacturing, large companies required suppliers to use EDI for all transactions,

eliminating tremendous amounts of paper and shortening the time and effort required to keep databases current. Value Added Networks (VANs) were typically used to carry EDI transactions, providing lower costs than dedicated connections such as leased lines, while offering a reliable and secure delivery service.

The Internet can provide the connectivity needed to support EDI at a substantial cost saving over VANs. However, the Internet doesn't provide the security services (integrity, confidentiality, non-repudiation) required for business EDI. Similar to electronic mail over the Internet, EDI transactions are vulnerable to modification, disclosure or interruption when sent over the Internet. The use of cryptography to provide the required security services has changed this, however, and many companies and government agencies are moving to Internet-based EDI.

4.10 Information Transactions

Providing information is a major and costly element of commerce. Such information may take a variety of forms:

- Static data, such as historic information, maps, etc.
- Corporate information, such as telephone numbers, addresses, organization charts, etc.
- Produce or service information
- Fee-based information services, such as news, periodical subscriptions, data base retrievals, stock quotes, etc.

Using the Internet to provide these services is substantially less expensive than using fax, telephone, or postal mail services. Potential customers can search for and retrieve information at their own pace without requiring expensive customer support services.

Typically, such information services use the World Wide Web as the underlying mechanism for providing information. Integrity and availability of the information provided are key security concerns that require security controls and policy.

4.11 Financial Transactions

In one form or another, computers and networks have been used to process financial transactions for decades. Electronic Funds Transfers are used bank to bank transactions, and Automated Teller Machines are used for consumer to bank transactions. Credit card authorizations and settlement processing is performed over telephone lines or data networks.

To maintain the security of these transactions, they have always been carried over private networks or been encrypted using the Data Encryption Standard. Similar to EDI over VANs, the connectivity options have been limited and the leased lines are expensive. Once again the Internet provides an opportunity for cost savings in electronic financial transactions.

There are three major classes of financial transactions and five major types of payment mechanisms:

Table 4.3 Financial Payments and Transactions

	Cash	Check	Debit	Credit	EFT

	Cash	Check	Debit	Credit	EFT
Business to Business		Primary			Secondary
Business to Consumer	Primary	Secondary	Secondary	Secondary	
Consumer to Consumer	Primary	Secondary			

The use of the Internet to carry these types of transactions replaces the physical presentation or exchange of cash, checks, or debit/credit cards with the electronic equivalent:

- Cash - there are a number of competing approaches to electronic cash under development. All methods use cryptography to create secure digital “wallets” to safely store digital currency. The transfer of electronic cash does not necessarily have to involve a financial institution as an intermediary.
- Checks - the banking industry is developing a standard for electronic checking, defining how the information carried on physical checks should be contained in an electronic message. Electronic checks will always involve a financial institution for transferring funds.
- Debit cards - Smart cards and stored value cards can be loaded with electronic currency in a variety of manners. Each transaction debits the appropriate amount until the card is empty. Stored value cards do not require financial institutions as intermediaries.
- Credit Cards - the major players in the credit card industry (Visa, Master Card, and American Express) have developed a standard for performing credit card transactions over public networks. Known as Secure Electronic Transactions, this standard supports the three-way transactions between the buyer, the seller, and the acquirer of the credit card debt, typically a bank. Electronic credit card transactions using SET will always involve a financial institution.
- Electronic Funds Transfer (EFT) - EFT uses cryptography to secure the transfer of funds between banks and other financial institutions. Consumers can authorize banks to send and receive payments via EFT for the consumer.

Each of these forms of electronic financial transactions involves the use of cryptography to provide for integrity, confidentiality, authentication, and non-repudiation.

4.12 High Availability

As use of the Internet becomes more critical to routine business operations, security controls protecting Internet connections often need to support requirements for high availability or non-stop operations. These requirements often have a major impact on security policy, requiring business decisions between the costs of redundant configurations versus the cost of temporarily operating without security controls.

A simple example is the firewall. A firewall can be a single point of failure - if the firewall goes down, the entire connection to the Internet can be lost for the duration of the failure. If temporary

loss of Internet connectivity does not have a major impact on business operations, the policy may be to simply halt Internet operations until the firewall is restored. For low risk profile organizations, the policy may allow the failed firewall to be bypassed for the duration of the outage. However, if the connectivity is critical, or for higher risk profile organizations, policy may require the acquisition and use of a firewall configured as a hot or cold spare. The business or mission side of the organization makes the tradeoff between the costs of each approach.

For very large organizations, performance may also dictate the use of multiple security controls, such as firewalls or authentication servers. For example, an organization supporting many thousands of external Internet users may need multiple T1 connections to the Internet, requiring multiple firewalls. Organizations with many thousands of internal users who tend to connect to the system simultaneously (early in the morning, right after lunch, etc.) may require multiple authentication servers to keep response times to acceptable levels.

Some of the key efforts in supporting high availability requirements are:

- Capacity planning - An interesting phenomenon is that as soon as a firewall is installed, users will swear the Internet connection is slower. Properly selected security controls such as firewalls will generally not be the bottleneck in system throughput. However, detailed capacity planning is critical, as security controls that do impact performance will quickly be bypassed. Firewall vendors' specifications should be derated at least 50% when modeling needed capacity, and any critical security control should have its performance profiled on a test network.
- Redundancy - For all but the lowest risk profile organizations, an on-line backup firewall is a necessity. Similarly, the use of authentication servers or secure remote access servers generally require the ability to rapidly switch in backup servers. Synchronization of policy is the key for the use of redundant backup security servers - all updates, backups, and modifications must be implemented on both systems, and the licensing for both systems must be kept current.
- Recovery - when a failed unit has been repaired and brought back on line careful configuration control is a must. The hardware and software configuration must be analyzed to assure that approved, current and patched versions of all products are running and that no unneeded services have been introduced or enabled during the repair process. Any debug features or system traps used in testing should be removed or disabled.

4.13 Ease of Use

The user population of many systems connected to the Internet may range from secretaries to scientists, from neophytes to nerds. A frequent business requirement is often that all applications be easy to use by the typical user population. This is not an easy requirement to quantify, but from a security perspective often gets translated as: "If security controls get in the way of people doing their jobs, we will figure out a way to bypass the security controls."

Two key elements of ease of use are reducing the number of times a user has to authenticate to the system and designing the interface to security controls to match the capabilities or preferences of the user population. These areas are discussed in the following sections.

4.14 Single Sign-on

In the course of performing daily tasks, a user might be forced to log on to many different computers and networks. Often, each system requires the user to enter a username and password. Since remembering multiple passwords is difficult for many users, this leads to passwords being written down (and often posted on PC monitors) or forgotten. Another user

reaction is to simply use the same password for all computer systems. However, different systems may have different rules for passwords, or may have different periods of validity for passwords, causing users to resort to once again writing down the various passwords.

Single Sign-on systems attempt to make the use of multiple passwords transparent to the user. This is accomplished in a variety of ways:

- Some SSO systems simply create scripts which contain the various username/password pairs and logon commands. This removes the burden from the user, but often transfers it to the administrative staff who often is required to maintain the scripts. Such scripts also require secure storage, as misuse would allow access to all systems for which the user has privileges.
- Other approaches to Single Sign-on, such as those based on Kerberos, use cryptographic techniques to forward user privileges to each network or server the user needs to access. These systems require the establishment and operation of privilege servers, as well as the integration of the SSO technology into each system to be accessed.

4.15 User Interface Design

The design of the user interface to Internet security functionality should be consistent with the user interface of other applications that will be used regularly by system users. When security controls are purchased off-the-shelf, or are embedded in off-the-shelf applications, the user interface to such security functionality will be outside the control of your organization. For internally developed applications it is important that the user interface be designed considering the perspective of the end user, not the security organization.

